PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
GEOFFREY K. GAVIN
1100 PEACHTREE STREET, #2800
ATLANTA, GA 30309-4530

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing *(day/month/year)* 03 SEP 2004
Applicant's or agent's file reference 39932 283893	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US04/09682	International filing date *(day/month/year)* 30 March 2004 (30.03.2004)
Applicant PATHFIRE, INC.	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 740 14 35

   For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   Shortly after the expiration of **18 months** *from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.*

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Matthew T Henning Telephone No. (703)305-3900

Form PCT/ISA/220 (January 2004) *(See notes on accompanying sheet)*

KS Docketing
Docketed for: 10/20/04
Entered on: 9/13/04
Initials: AH
Previously Entered:

RECEIVED
SEP 08 2004

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 39932 283893	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US04/09682	International filing date (*day/month/year*) 30 March 2004 (30.03.2004)	(Earliest) Priority Date (*day/month/year*) 02 April 2003 (02.04.2003)
Applicant PATHFIRE, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
      ☐ The international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.
2. ☐ **Certain claims were found unsearchable** (See Box No. II)
3. ☐ **Unity of invention is lacking** (See Box No. III)
4. With regard to the **title**,
   ☒ the text is approved as submitted by the applicant.
   ☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   ☐ the text is approved as submitted by the applicant.
   ☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. ____
      ☐ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☒ none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/09682

Box IV TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

The abstract contains statements on the alleged merits or value of the claimed invention and on its speculative application (PCT Rule 8.1(c)).
The following is a new abstract:
A method for securely transmitting data involves generating keys depending on previous keys and additional information, such as a password, in order to create a pseudo one-time pad. The data is encrypted using the pseudo one-time pad prior to transmission. Only the initial key and minimal additional data are transferred between the sender and receiver in order to synchronize the keys.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/09682

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 11/30, 12/14; H04L 9/00 9/32; H04K 1/04, 1/06

US CL : 713/200, 201, 202; 380/36, 37, 44

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201, 202; 380/36, 37, 44

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,307,940 B1 (Yamamoto et al.) 23 October 2001 (23.10.2001), Whole Document,	1-2
---	Especially Col. 2, Col. 18 - Col. 22, and Figure 23	---
Y		3-5
Y	US 5,412,730 A (Jones) 2 May 1995 (02.05.1995), Fig. 1, Col. 1, and Col. 4.	3-4
Y	Schneier, Bruce, "Applied Cryptography", 1996, Second Edition, pages 353-354.	4
Y	US 5,680,460 A (Tomko et al.) 21 October 1997 (21.10.1997) Col. 2	5

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 August 2004 (19.08.2004)	03 SEP 2004
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Matthew T Henning Telephone No. (703)305-3900

Form PCT/ISA/210 (second sheet) (January 2004)

PATENT COOPERATION TREAT

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GEOFFREY K. GAVIN
1100 PEACHTREE STREET, #2800
ATLANTA, GA 30309-4530

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	03 SEP 2004
Applicant's or agent's file reference 39932 283893	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US04/09682	30 March 2004 (30.03.2004)	02 April 2003 (02.04.2003)

International Patent Classification (IPC) or both national classification and IPC

IPC(7): G06F 11/30, 12/14; H04L 9/00 9/32; H04K 1/04, 1/06 and US Cl.: 713/200, 201, 202; 380/36, 37, 44

Applicant

PATHFIRE, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I — Basis of the opinion
- ☐ Box No. II — Priority
- ☐ Box No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV — Lack of unity of invention
- ☒ Box No. V — Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI — Certain documents cited
- ☐ Box No. VII — Certain defects in the international application
- ☐ Box No. VIII — Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Matthew T Henning Telephone No. (703)305-3900

Form PCT/ISA/237 (cover sheet) (January 2004)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/09682

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ This opinion has been established on the basis of a translation from the original language into the following language _____, which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ in written format

☐ in computer readable form

c. time of filing/furnishing

☐ contained in international application as filed.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/09682

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 3-5	YES
	Claims 1-2	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-5	NO
Industrial applicability (IA)	Claims 1-5	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:

Claims 1-2 lack novelty under PCT Article 33(2) as being anticipated by Yamamoto et al. Yamamoto et al. disclosed dividing a message to be encrypted into blocks and setting a number of blocks to be encrypted with each key (See Yamamoto et al. Col. 18 Paragraph 4 Lines 9-12). Yamamoto et al. further disclosed encrypting the first set of blocks with a first key (Col. 18 Paragraph 5 Lines 13-14). Yamamoto et al. depicted and disclosed generating new keys from previous keys and an initial value (See Fig. 23 and Col. 2 Lines 10-37) and encrypting the second set of blocks with the second key (See Col. 18 Paragraph 5 Lines 14-15). Yamamoto et al. also disclosed after encrypting the message, sending the message to the receiver (See Col. 18 Paragraph 5 lines 15-17). Yamamoto et al. further disclosed removing the keys once they were used (See Fig. 14 and Col. 22 Lines 12-13). Yamamoto et al. also disclosed producing a key for each set of blocks and using the key to encrypt that set of blocks (See Col. 20 Lines 12-15).

Claim 3 lacks an inventive step under PCT Article 33(3) as being obvious over Yamamoto et al. in view of Jones. Yamamoto et al. did disclose using a password (initial value) and shift points (block lengths and number of blocks per key) to create keys for encrypting (See Yamamoto et al. Figure 23 and Col. 18 Paragraphs 4-5). Yamamoto also disclosed transmitting the initial value to the receiver (See Yamamoto et al. Col. 18 Paragraph 5 Lines 1-2) but failed to disclose transmitting the shift points to the receiver. Jones teaches that in order to synchronize the key generators in a key changing system and to accurately decipher the transmitted data, an interval number is transmitted between the sender and the receiver (See Jones Fig. 1 and Col. 1 Lines 54-58 and Col. 4 Lines 3-19). It would have been obvious to one of ordinary skill to employ the teachings of Jones to the cipher of Yamamoto et al. by transmitting the interval value from the sender to the receiver. This would have been obvious because one of ordinary skill would have been motivated to allow the intended receiver of the encrypted message to properly decipher the message.

Claim 4 lacks an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Schneier. Yamamoto et al. disclosed a password (See Yamamoto et al. Figure 23 and Col. 18 Paragraphs 4-5) and Jones disclosed an iteration value and symbol value (See Jones Col. 1 Lines 54-58). However, Yamamoto and Jones failed to disclose the use of a hash algorithm to create the key. Schneier teaches that using a one-way hash function as the key generator for a block cipher causes the cipher to run almost as fast as the hash function itself (See Schneier Page 353 Message Digest Cipher Lines 1-4 and Page 354 Figure 14.5). It would have been obvious to one of ordinary skill to employ the teachings of Schneier to the combination of Yamamoto et al. and Jones by using a hash function to create the keys. This would have been obvious because one of ordinary skill would have been motivated to create a cipher that is both simple and fast.

Claim 5 lacks an inventive step under PCT Article 33(3) as being obvious over Yamamoto et al. in view of Tomko et al. Yamamoto failed to disclose the use of digital media as the first key. Tomko et al. teaches the use of biometric data, such as a fingerprint, as input to a key generator (See Tomko et al. Col. 2 Paragraphs 2-3). It would have been obvious to one of ordinary skill to employ the teachings of Tomko in the invention of Yamamoto et al. in order to generate the first key of the cipher. This would have been obvious because one of ordinary skill would have been motivated to provide an extremely secure initial key, which was readily accessible, yet unknown to the user.

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under Article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article," "Rule" and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

What parts of the international application may be amended ?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Preliminary Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When ? Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments ?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How ? Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments ?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

(i) the claim is unchanged;

(ii) the claim is cancelled;

(iii) the claim is new;

(iv) the claim replaces one or more claims as filed;

(v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."
2. [Where originally there were 15 claims and after amendment of all claims there are 11]:
"Claims 1 to 15 replaced by amended claims 1 to 11."
3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."
4. [Where various kinds of amendments are made]:
"Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under Article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments and any accompanying statement, under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the time of filing the amendments (and any statement) with the International Bureau, also file with the International Preliminary Examining Authority a copy of such amendments (and of any statement) and, where required, a translation of such amendments for the procedure before that Authority (see Rules 55.3(a) and 62.2, first sentence). For further information, see the Notes to the demand form (PCT/IPEA/401).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see the *PCT Applicant's Guide*, Volume II.